CYBER-SECURITY POLICY

Policy Statement

Sea-Tech Marine Construction Ltd (Sea-Tech) has identified Cyber Security as a major risk to the organisation. As a principle, our procedures and practices aim at protecting the company's information and data assets from all threats, whether internal or external, deliberate, or accidental. Sea-Tech has invested in technical security measures to ensure there is the very best processes in place to protect the organisation and its information.

All laptops are to be password protected by an 8-character password. The operating system should prompt password changes on a regular basis. Some points to remember when creating a secure password are:

- Choose a password that includes upper- and lower-case letters, numbers and includes special characters (!@~*)
- Always keep passwords secret and do not share them with other employees
- Do not reuse old passwords
- Do not let any other persons use your IT equipment, it is your responsibility, and you may be liable if a breach occurs.

All company issued IT equipment is of a certain specification and must not be tampered with in any way. This includes switching off any of the security measures, antivirus software, firewalls, web filtering, encryption, or any automatic updates.

Should you suspect a security breach, you have a duty to report it immediately to the CEO and the designated deputy for action and investigation. If it is a suspicious email, do not open it or any attachments until it has been deemed safe, by IT support, to do so.

If there is a Guest Wi-Fi facility for visitor use at your location, they are not entitled to use the employee network and any unauthorised use will be identified and disconnected immediately.

No unauthorised software is to be downloaded onto company owned IT equipment. Any requests for software to be added to the equipment must be made to the Sea-Tech Management in the first instance who will assess and approve where necessary. This will then be installed by the Company's IT Provider, 'Cyber PC'.

No visitors or contract personnel are to be given access to the Sea-Tech networks, its systems or hardware without the explicit permission of the CEO.

All users, including staff and contractors need to be diligent and not connect to unknown websites, download large files from unknown sources or access any inappropriate content as detailed in ST-p-020 Internet and Email Usage Policy.

The use of USB portable hard drives by external parties is prohibited within Sea-Tech where this can lead to access of information that details IP or is of a confidential or commercial nature

SEA TECH
MARINE CONSTRUCTION

CYBER-SECURITY POLICY

Only senior management team members (Operations Manager and above) are authorized to use USB Drives, with the exception of site / project managers who may authorize staff to use USB Drives solely for the purpose of documentation of operational tasks. This includes daily reports, photographs, and videos. Any use of USB drives beyond the above must receive authorization from a senior staff member.

All employees will be given an understanding of Sea-Techs Cyber Safety protocols, this will be carried out upon joining the organisation as part of the new employee induction.

This Sea-Tech Policy document has been established to address the above and aims to give employees guidance on appropriate do's and don'ts, together with areas of strict procedural requirements where business, legal dictates or asset protection needs apply. They have been written to avoid being over prescriptive whilst still meeting our obligations and through use and feedback they can of course be modified for improvement or as legal requirements change.

It is important that all employees understand the content of this policy and will comply fully with its content. Should obvious and wilful disregard be displayed then disciplinary action will result in accordance with the Company's standard procedures. This may be for any of the following reasons:

- Malicious or illegal activity conducted using company equipment or on the company network
- Accessing inappropriate material such as adult or illegal content using company equipment or on the company network
- Excessive personal use of company equipment during working hours
- Removing data or information from the drives or company premises without permission, i.e., use of USB hard drives
- The removal of technical cyber security systems such as antivirus software, firewalls etc.
- Any use of the company equipment prohibited in this policy
- Failing to report suspicious activity, emails, or security breaches
- Any unauthorised use of company owned equipment by visitors or contract personnel without prior permission
- Any employee found to be misusing the company equipment, IT systems or involved in a cyber security breach will be reported to the CEO or his designated delegate and may result in action in accordance with Sea-Techs Disciplinary Procedures

I would ask all of you to apply this policy rigorously for the protection of the company, our employees and yourself.

Robbie Hartog
CEO
9th June 2021